REMARKS/ARGUMENTS

I. Introduction:

Claims 1-20, 22-24, 26, and 29-44 are pending.

II. Claim Rejections Under 35 U.S.C. 102:

Claims 1-20, 22-24, 26, and 29-44 stand rejected under 35 U.S.C. 102(e) as being unpatentable over U.S. Patent No. 6,735,702 (Yavatkar et al.).

Applicant respectfully submits that the pending claims are not anticipated by Yavatkar et al. Reconsideration of the rejections in the Office Action dated April 27, 2005 is requested.

Yavatkar et al. is directed to a method and system for diagnosing network intrusion. The system monitors network traffic and, when a network condition is detected, gathers information about the traffic by launching an agent. Two types of agents are used to collect information. The first is a watchdog agent which is positioned at a network node. When the watchdog agent detects a network attack, it creates a bloodhound agent, which analyzes attack traffic by moving through the network and gathering information. After gathering information, the bloodhound agent may report back to the watchdog agent, which, in turn may report to a human operator. The operator can then shut down a gateway or install a firewall to block traffic.

Applicant's invention, as set forth in the claims, is particularly advantageous in that it shares filter information between a downstream node and an upstream node such that only traffic that would be forwarded to the requesting downstream node is affected. Importantly, this limits use of the system by an attacker as a means for

carrying out a denial of service attack, for example. Furthermore, applicant's invention, as set forth in claim 1, analyzes new data received at the first network device and sends filter information to the second network device so that it can refine its filter, as needed.

Yavatkar et al. do not: send information on a filter installed at a first network device to a second network device; request the second network device to install a filter so that data is filtered closer to a source of the data; send routing information from the first network device to the second network device; analyze new data received from the second network device at the first network device; or send filter information to the second network device based on the analyzed data, as set forth in claim 1.

The system of Yavatkar et al. does not send filter information between devices or request an upstream device to install a filter. Yavatkar et al. send agents between nodes to collect information and diagnose a network intrusion. The only information sent back from a bloodhound agent to a watchdog agent is information identifying an attack. One agent does not request another agent installed on an upstream node to filter data or send filter information so that the node knows what to filter. In rejecting the claims, the Examiner identifies nodes such as node 30 as a first network device and node 48 as a second network device. As noted at col. 7, lines 42-45, node 48 is a gateway providing network access to other networks. Network device 30 does not have any input as to what traffic node 48 filters.

Furthermore, Yavatkar et al. do not send routing information from the first network device to the second network device so that a filter installed on the second network device filters traffic forwarded to the first network device without filtering traffic to other downstream nodes, as required by claim 1. As discussed above, node 48 of Yavatkar et al. does not filter traffic based on any information received from the first network device.

The second network device (identified by the Examiner as node 48) does not send new data back to the first network device so that the first network device can analyze the data and send new filter information to the second device. As a further example, the watchdog agent of Yavatkar et al. does not analyze data received from the bloodhound agent and respond with new filter information. As previously noted, the bloodhound agent simply sends information it gathers on a network attack back to the watchdog agent. The watchdog agent does not respond to the bloodhound agent. Therefore, there is no analysis performed at the network devices in order to refine filters. And, as discussed above, the network devices or agents do not send filter information back and forth, thus there is no sending of filter information so that a network device can refine a filter. This feature of applicant's invention allows a downstream device to receive filter statistics from an upstream device. This is important because once the filter is installed on the upstream device, the downstream device will not see the traffic. If the downstream device determines that the filter is no longer required based on the analyzed flow, the device can send a message to the upstream device to remove or refine its filter.

Accordingly, claim 1 is submitted as not anticipated by Yavatkar et al. Claims 2-12, 22-24, 26, and 30-44, depending either directly or indirectly from claim 1, are submitted as patentable for at least the same reasons as claim 1.

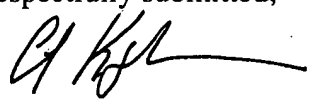
Claims 13, 18, and 19, and the claims depending therefrom, are submitted as patentable for at least the reasons discussed above with respect to claim 1.

III. Conclusion:

For the foregoing reasons, Applicant believes that all of the pending claims are in condition for allowance and should be passed to issue. If the Examiner feels that a

telephone conference would in any way expedite prosecution of the application, please do not hesitate to call the undersigned at (408) 399-5608.

Respectfully submitted,



Cindy S. Kaplan
Reg. No. 40,043

P.O. Box 2448
Saratoga, CA 95070
Tel: 408-399-5608
Fax: 408-399-5609